

**HIPAA
PRIVACY
AND
SECURITY RULES**

**BUSINESS ASSOCIATE
AGREEMENT**

BETWEEN

Stewart C. Miller & Co., Inc.
(Business Associate)

AND

City of West Lafayette Flexible Spending Plan
(Covered Entity)

TABLE OF CONTENTS

PREAMBLE	1
I. DEFINITIONS	1
SECTION 1.01 - "BREACH"	1
SECTION 1.02 - "BUSINESS ASSOCIATE"	2
SECTION 1.03 - "COVERED ENTITY"	2
SECTION 1.04 - "ELECTRONIC PROTECTED HEALTH INFORMATION"	2
SECTION 1.05 - "ELECTRONIC MEDIA"	2
SECTION 1.06 - "HIPAA"	2
SECTION 1.07 - "INDIVIDUAL"	3
SECTION 1.08 - "NOTICE OF BREACH"	3
SECTION 1.09 - "PRIVACY RULE"	3
SECTION 1.10 - "PROTECTED HEALTH INFORMATION" OR "PHI"	3
SECTION 1.11 - "REQUIRED BY LAW"	3
SECTION 1.12 - "SECRETARY"	3
SECTION 1.13 - "SECURITY INCIDENT"	3
SECTION 1.14 - "SECURITY RULE"	3
SECTION 1.15 - "UNSECURED PHI"	3
II. SPECIFIC REQUIREMENTS	4
SECTION 2.01 - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE	4
SECTION 2.02 - PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE	6
SECTION 2.03 - OBLIGATIONS OF COVERED ENTITY	7
III. OTHER TERMS	7
SECTION 3.01 - AMENDMENTS IN WRITING	7
SECTION 3.02 - AMENDMENT TO COMPLY WITH HIPAA	7
SECTION 3.03 - APPLICABLE LAW AND FORUM	8
SECTION 3.04 - AUTHORITY	8
SECTION 3.05 - DATA OWNERSHIP	8
SECTION 3.06 - INDEMNIFICATION	8
SECTION 3.07 - INTERPRETATION	8
SECTION 3.08 - NOTICES	8
SECTION 3.09 - REGULATORY REFERENCES	8
SECTION 3.10 - SURVIVAL	8
SECTION 3.11 - THIRD PARTY RIGHTS	9
SECTION 3.12 - WAIVER	9
SECTION 3.13 - ACCESS TO COVERED ENTITY INFORMATION SYSTEMS	9
IV. TERM AND TERMINATION	9
SECTION 4.01 - TERM OF AGREEMENT	9
SECTION 4.02 - TERMINATION FOR CAUSE	9
SECTION 4.03 - EFFECT OF TERMINATION	10
SIGNATURE PAGE	11

PREAMBLE

This Business Associate Agreement (“Agreement”) is entered into this ____ day of _____, 2010 by and between the **City of West Lafayette Flexible Spending Plan** (“Covered Entity”) and **Stewart C. Miller & Co., Inc.** (“Business Associate”).

WHEREAS, Covered Entity is in the business of providing health care services;

WHEREAS, Business Associate is in the business of providing administrative services to the Covered Entity;

WHEREAS, Business Associate may, in the course of providing such services, have certain Protected Health Information (as defined herein) disclosed to it;

WHEREAS, Business Associate and Covered Entity are entering into this Agreement to set forth Business Associate’s obligations with respect to its handling of the Protected Health Information; and

WHEREAS, the law governing the duties and relationships between Covered Entities and Business Associates was changed by the *American Recovery and Reinvestment Act of 2009 (ARRA)* and the parties desire to execute a new Business Associate Agreement reflecting these changes,

NOW THEREFORE, for mutual consideration, the sufficiency of which is acknowledged by both parties, the parties agree as follows:

I. DEFINITIONS

In general, the terms and language herein are to be understood as such are commonly used or, as applicable, as used in light of the Privacy and/or Security Rule, as amended, and any guidance issued thereunder.

Section 1.01 -“Breach”

“Breach” means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purposes of this definition, *“compromises the security or privacy of the protected health information”* means *“poses a significant risk of financial, reputational, or other harm to the individual.”* A use or disclosure of PHI that does not include the identifiers listed at 45 C.F.R. 164.514(e)(2), date of birth, and zip code does not “compromise” the security or privacy of the PHI and is not a Breach.

The term Breach excludes:

- (i) Any unintentional acquisition, access, or use of PHI by a person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

- (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Section 1.02 - "Business Associate"

"Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR 160.103.

Section 1.03 - "Covered Entity"

"Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR 160.103.

Section 1.04 - "Electronic Protected Health Information"

"Electronic Protected Health Information" (or, "e-PHI" or "E-PHI") shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR 160.103 and generally means protected health information ("PHI") that is transmitted or maintained in Electronic Media.

Section 1.05 - "Electronic Media"

"Electronic Media" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR 160.103 and shall mean:

- (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Section 1.06 - "HIPAA"

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

Section 1.07 - "Individual"

"**Individual**" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a "personal representative" in accordance with 45 CFR 164.502(g).

Section 1.08 - "Notice of Breach"

"**Notice of Breach**" means the notice required to be given by Covered Entities to individuals and others under the regulation for *Breach Notification for Unsecured Protected Health Information* 45 C.F.R. Secs. 164.400-164.414, as well as the notice required to be given to Covered Entities by their Business Associates of any such Breach.

Section 1.09 - "Privacy Rule"

"**Privacy Rule**" shall mean the HIPAA Regulation that is codified at 45 CFR 160 and 164, Subparts A and E.

Section 1.10 - "Protected Health Information" or "PHI"

"**Protected Health Information**" or "**PHI**" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term at 45 CFR 160.103. E-PHI is a subset of PHI.

Section 1.11 - "Required By Law"

"**Required By Law**" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

Section 1.12 - "Secretary"

"**Secretary**" shall mean the Secretary of the Department of Health and Human Services or his designee.

Section 1.13 - "Security Incident"

"**Security Incident**" shall have the meaning set forth in 45 CFR 164.304, as amended from time to time, and generally means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with systems operations in an information system.

Section 1.14 - "Security Rule"

"**Security Rule**" shall mean the HIPAA Regulation that is codified at 45 CFR 160 and 164, Subparts A and C.

Section 1.15 - "Unsecured PHI"

"**Unsecured PHI**" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the

Secretary of HHS in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS web site. Such technology or methodology is also discussed at 74 FR 42742.

II. SPECIFIC REQUIREMENTS

Section 2.01 - Obligations and Activities of Business Associate

Business Associate agrees to take the following actions and any other actions that may be required under the Privacy and Security rules:

- A. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.
- B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- C. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware. Pursuant to 45 C.F.R. Sec. 164.410, Business Associate also agrees to provide notice to the Covered Entity of any Breach (as defined herein) of Unsecured PHI to the Covered Entity without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification required by this paragraph shall include, to the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach.

The Business Associate shall provide the Covered Entity with any other available information that the Covered Entity is required to include in its notification to an individual under 45 C.F.R. Sec. 164.404(c) at the time of the notification required given to the Covered Entity or promptly thereafter as information becomes available.

The Business Associate shall bear burden of demonstrating that all notifications to the Covered Entity were made as required by C.F.R. Sec. 164.410 or that the use or disclosure did not constitute a Breach of Unsecured PHI. The Business Associate shall retain the records of its investigation and analysis of any suspected or known Breach of Unsecured PHI and shall make such records available to the Covered Entity or HHS as requested.

- D. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- E. Business Associate agrees to make available Protected Health Information in accordance with 45 CFR 164.524;

- F. Business Associate agrees to make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with 45 CFR 164.526;
- G. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner agreed upon by the parties, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. In order to fulfill this obligation, Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- H. Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner agreed upon by the parties or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- I. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- J. Business Associate agrees that, it has or will timely implement the requirements of the HIPAA Security Rule, as amended by *ARRA*:
 - 1. Implementing administrative (45 C.F.R. 164.308) , physical (45 C.F.R. 164.310), and technical safeguards (45 C.F.R. 164.312) consistent with (and as required by) the HIPAA Security Rule that reasonably protect the confidentiality, integrity, and availability of e-PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity. Business Associate also agrees be compliant with the policies and procedures and documentation requirements (45 C.F.R. 164.314) applicable to Business Associates under *ARRA*, and the guidance issued thereunder;
 - 2. Ensuring that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect such information;
 - 3. Reporting and tracking all Security Incidents as described below:
 - a. Business Associate shall report to the Covered Entity any Security Incident that results in (i) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's e-PHI, or (ii) interference with Business Associate's system operations in Business Associate's

information systems or to which Business Associate becomes aware within a reasonable period of time thereafter;

- b. For any other Security Incident, Business Associate shall aggregate the data and provide such reports on a quarterly basis or as the Covered Entity and Business Associate otherwise agree; and
- 4. Making Business Associate's policies and procedures and documentation required by the HIPPA Security Rule related to these safeguards available to the Secretary of U.S. Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Security Rule.
- K. Business Associate agrees to take all reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from a Security Incident, including any reasonable steps recommended by the Covered Entity. Business Associate agrees to provide to the Covered Entity all information concerning such disclosure or breach as may be reasonably requested by the Covered Entity.

Section 2.02 - Permitted Uses and Disclosures of PHI by Business Associate

A. General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the underlying service contract between the parties, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

B. Specific Use and Disclosure Provisions

- 1. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate, to carry out the legal responsibilities of the Business Associate or to provide data aggregation services relating to the health care operations of the Covered Entity.
- 2. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that such disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Section 2.03 - Obligations of Covered Entity

A. Provisions for Covered Entity To Inform Business Associate of Privacy Practices and Restrictions

1. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
2. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

B. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

III. OTHER TERMS

Section 3.01 - Amendments in Writing

Any amendment to this Agreement shall not be binding on either of the parties to this Agreement unless such amendment is in writing and executed by the party against whom enforcement is sought.

Section 3.02 - Amendment to Comply with HIPAA

The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and Security Rule. In the event of a change in the law relative to the rights, duties and obligations of the parties under this Agreement or applicable law, the parties agree to operate in accordance with the law until such time as a formal amendment to this Agreement may be made, as needed.

Section 3.03 - Applicable Law and Forum

This Agreement shall be interpreted and construed in accordance with the laws of the State of Indiana. Any action arising under or relating to this Agreement shall be brought in the federal or state courts located in the jurisdiction of the Fund, or as agreed upon by the parties. Each party hereto consents to the jurisdiction of the foregoing courts.

Section 3.04 - Authority

Each party has full power and authority to enter into and perform this Agreement, and the person signing this Agreement on behalf of each party has been properly authorized and empowered to enter into this Agreement.

Section 3.05 - Data Ownership

Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Health Information.

Section 3.06 - Indemnification

The Covered Entity and Business Associate each agrees to defend, hold harmless and indemnify the other from any and all claims, liabilities, damages or judgments asserted against, imposed upon or incurred by the other that arise out of its negligence or willful misconduct.

Section 3.07 - Interpretation

Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules. In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of the HIPAA Privacy and Security Rules, as may be expressly amended from time to time by the Department of Health and Human Services (HHS) or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the Parties, the interpretation of HHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence.

Section 3.08 - Notices

Any notices required or permitted under this Agreement shall be in writing and delivered in person or sent by registered or certified mail, return receipt requested, proper postage prepaid, properly addressed to the address of the addressee set forth hereinafter or to such other more recent address of the addressee of which the sending party has received written notice.

Section 3.09 - Regulatory References

A reference in this Agreement to a section in the Privacy and/or Security Rule means the section as in effect or as amended.

Section 3.10 - Survival

The respective rights and obligations of Business Associate under Section 4.03 of this Agreement shall survive the termination of this Agreement.

Section 3.11 - Third Party Rights

Except as expressly provided in the HIPAA Privacy and/or Security Rule or this Agreement, this Agreement does not create any rights in third parties.

Section 3.12 - Waiver

No delay or omission on the part of either party in exercising any right hereunder shall operate as a waiver of such right or of any other right under this Agreement. A waiver on any one occasion shall not be construed as a bar to or waiver of any right or remedy on any further occasion. The election of either party of a particular remedy on default will not be exclusive of any other remedy, and all rights and remedies of the parties hereto will be cumulative.

Section 3.13 - Access to Covered Entity Information Systems

If Business Associate is provided access to any of the Covered Entity's information system or network containing any Electronic PHI, Business Associate agrees to comply with all of the Covered Entity's policies for access to and use of information from the information systems or network, to the extent the Covered Entity has provided or informed the Business Associate of such policies.

IV. TERM AND TERMINATION

Section 4.01 - Term of Agreement

The Term of this Agreement shall be effective as of **January 1, 2010**, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. This Agreement shall supersede the prior Business Associate Agreement executed between the parties on the date this revised Agreement is fully executed, but does not create a "termination" triggering any of the above duties under a termination.

Section 4.02 - Termination for Cause

Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- A. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
- B. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
- C. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

Section 4.03 - Effect of Termination

- A. Except as provided in paragraph B. of this Section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
- B. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon the parties' agreement that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

SIGNATURE PAGE

COVERED ENTITY

By:_____

Dated

Title:_____

BUSINESS ASSOCIATE

By:_____

Dated

Title: Stewart C. Miller, President